Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - AhnLab V3 Antivirus Arbitrary Code Execution
  - Comersus BackOffice Plus Cross-Site Scripting
  - Kerio Personal Firewall and Server Firewall Denial of Service
  - **Microsoft Client Service for NetWare Arbitrary Code Execution (Updated)**
  - **Microsoft DirectX DirectShow Arbitrary Code Execution (Updated)**
  - **Microsoft Internet Explorer Arbitrary Code Execution (Updated)**
  - **Microsoft Windows FTP Client Arbitrary File Control (Updated)**
  - **Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service (Updated)**
  - **Microsoft Windows Plug and Play Arbitrary Code Execution (Updated)**
  - **Microsoft Windows Shell Arbitrary Code Execution (Updated)**
  - MailSite Express Arbitrary Code Execution
  - Typsoft FTP Server Denial of Service
  - VERITAS NetBackup Arbitrary Code Execution
- UNIX / Linux Operating Systems
  - Clam Anti-Virus ClamAV OLE2 File Handling Denial of Service
  - Flexbackup Insecure Temporary File Creation
  - Gentoo Linux Multiple Packages Insecure RUNPATH
  - **GNU GZip Directory Traversal (Updated)**
  - **GNU Texinfo Insecure Temporary File Creation (Updated)**
  - **GNU GZip File Permission Modification (Updated)**
  - **Graphviz Insecure Temporary File Creation (Updated)**
  - **Grip CDDB Query Buffer Overflow (Updated)**
  - HP-UX Itanium Denial of Service
  - HP-UX FTP Server Directory Listing
  - HP-UX LPD Arbitrary Command Execution
  - **HylaFAX Insecure Temporary File Creation (Updated)**
  - **IBM AIX Multiple Buffer Overflows (Updated)**
  - IBM AIX LSCFG Insecure Temporary File Creation
  - **KDE KOffice KWord RTF Remote Buffer Overflow (Updated)**
  - **Marc Lehmann Convert-UUlib Perl Module Buffer Overflow (Updated)**
  - **Multiple Vendors TLS Plaintext Password (Updated)**
  - **Multiple Vendors Cfengine Insecure Temporary Files (Updated)**
  - **Zlib Compression Library Buffer Overflow (Updated)**
  - **Multiple Vendors GDB Multiple Vulnerabilities (Updated)**
  - Multiple Vendors Linux Kernel Console Keymap Arbitrary Command Injection
  - Multiple Vendor WGet/Curl NTLM Username Buffer Overflow
  - **Multiple Vendors OpenSSL Insecure Protocol Negotiation (Updated)**
  - **Multiple Vendors XNTPD Insecure Privileges (Updated)**
  - Multiple Vendors OpenWBEM Multiple Unspecified Remote Buffer Overflows
  - Multiple Vendors NetPBM Buffer Overflow
  - **Multiple Vendors XFree86 Pixmap Allocation Buffer Overflow (Updated)**
  - **Multiple Vendors CDDB Client Format String (Updated)**
  - **Net-SNMP Protocol Denial Of Service (Updated)**
  - **Net-SNMP Fixprox Insecure Temporary File Creation (Updated)**
  - **PADL Software PAM_LDAP Authentication Bypass (Updated)**
  - **PCRE Regular Expression Heap Overflow (Updated)**
  - **PHPMyAdmin File Include (Updated)**
  - **slocate Long Path Denial of Service (Updated)**
  - **Sun Solaris Xsun & Xprt Elevated Privileges (Updated)**
  - Sun Solaris Denial of Service & Information Disclosure
  - Sun Solaris Proc Filesystem Denial of Service
  - **Sun Solaris UFS Local Denial of Service (Updated)**
  - **UW-imapd Denial of Service and Arbitrary Code Execution (Updated)**
  - **Xloadimage NIFF Image Buffer Overflow (Updated)**
  - Yapig Cross-Site Scripting & HTTP POST Requests Validity
  - **Ruby Safe Level Restrictions Bypass (Updated)**
- Multiple Operating Systems
  - AbiWord Stack-Based Buffer Overflows
  - Accelerated Mortgage Manager SQL Injection

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
AhnLab V3 AntiVirus V3Pro 2004 6.0.0.457,	A buffer overflow vulnerability has been reported in V3 AntiVirus that could let remote malicious users execute arbitrary code. Upgrade to version 6.0.0.488 using the applications	AhnLab V3 Antivirus Arbitrary Code Execution	High	Secunia, Advisory: SA16851, October 13, 2005

V3Net for Windows Server 6.0.0.457, MyV3 with AzMail.dll 1.3.11.15	Smart Update. Currently we are not aware of any exploits for this vulnerability.			
Comersus Open Technologies BackOffice Plus	An input validation vulnerability has been reported in BackOffice Plus that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Comersus BackOffice Plus Cross-Site Scripting	Medium	Security Tracker, Alert ID: 1015064, October 17, 2005
Kerio Technologies Personal Firewall 4.2, Server Firewall 1.1.1	A vulnerability has been reported in Kerio Personal Firewall and Server Firewall that could let local malicious users cause a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Kerio Personal Firewall and Server Firewall Denial of Service	Low	Security Focus, ID: 15094, October 13, 2005
Microsoft Client Service for NetWare	A buffer overflow vulnerability has been reported in Client Service for NetWare that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-046.mspx **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** Currently we are not aware of any exploits for this vulnerability.	Microsoft Client Service for NetWare Arbitrary Code Execution CVE-2005-1985	High	Microsoft, Security Bulletin MS05-046, October 11, 2005 **Avaya, ASA-2005-214, October 11, 2005**
Microsoft DirectX DirectShow 7.0 to 9.0c	A buffer overflow vulnerability has been reported in DirectX DirectShow that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** Currently we are not aware of any exploits for this vulnerability.	Microsoft DirectX DirectShow Arbitrary Code Execution CVE-2005-2128	High	Microsoft, Security Bulletin MS05-050, October 11, 2005 USCERT, VU#995220 Technical Cyber Security Alert TA05-284A, October 11, 2005 **Avaya, ASA-2005-214, October 11, 2005**
Microsoft Internet Explorer 5.01, 5.5, 6.0	A vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-052.mspx **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** An exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2005-2127	High	Microsoft, Security Bulletin MS05-052, October 11, 2005 Technical Cyber Security Alert TA05-284A, October 11, 2005 **Avaya, ASA-2005-214, October 11, 2005** **USCERT, VU#680526, VU#959049, VU#740372, VU#898241**
Microsoft Windows FTP Client	An input validation vulnerability has been reported in Windows FTP Client that could let remote malicious users to obtain arbitrary file control. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-044.mspx **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** A Proof of Concept exploit script has been published.	Microsoft Windows FTP Client Arbitrary File Control CVE-2005-2126	Medium	Microsoft, Security Bulletin MS05-044, October 11, 2005 **Avaya, ASA-2005-214, October 11, 2005** **USCERT, VU#415828**

Microsoft Windows Microsoft Distribution Transaction Coordinator (MSDTC) and COM+	A buffer overflow vulnerability has been reported in Windows MSDTC and COM+ that could let local or remote malicious users execute arbitrary code, obtain elevated privileges or cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx **Vendor has identified potential issues associated with fix:** **http://www.microsoft.com/technet/security/advisory/909444.mspx** **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service CVE-2005-1978 CVE-2005-1979 CVE-2005-1980 CVE-2005-2119	High	Microsoft, Security Bulletin MS05-051, October 11, 2005 US-CERT VU#180868, US-CERT VU#950516 Technical Cyber Security Alert TA05-284A, October 11, 2005 **Microsoft, Security Advisory 909444, October 14, 2005** **Avaya, ASA-2005-214, October 11, 2005**
Microsoft Windows Plug and Play	A buffer overflow vulnerability has been reported in Windows Plug and Play that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-047.mspx **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Plug and Play Arbitrary Code Execution CVE-2005-2120	High	Microsoft, Security Bulletin MS05-047, October 11, 2005 USCERT, VU#214572 Technical Cyber Security Alert TA05-284A, October 11, 2005 **Avaya, ASA-2005-214, October 11, 2005**
Microsoft Windows Shell	A vulnerability has been reported in Windows Shell that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-049.mspx **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-214.pdf** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Shell Arbitrary Code Execution CVE-2005-2117 CVE-2005-2118 CVE-2005-2122	High	Microsoft, Security Bulletin MS05-049, October 11, 2005 USCERT, VU#922708 Technical Cyber Security Alert TA05-284A, October 11, 2005 **Avaya, ASA-2005-214, October 11, 2005**
Rockliffe MailSite Express 6.1.20	A vulnerability has been reported in MailSite Express that could let remove malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	MailSite Express Arbitrary Code Execution	High	Security Tracker, Alert ID: 1015063, October 17, 2005
Typsoft FTP Server 1.11	A vulnerability has been reported in Typsoft FTP Server that could let remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Typsoft FTP Server Denial of Service	Low	Secunia, Advisory: SA17196, October 14, 2005
Veritas NetBackup Data and Business Center 4.5FP, 4.5MP, Client/ Enterprise/ Server 5.0, 5.1, 6.0	A vulnerability has been reported in NetBackup that could let remote malicious users execute arbitrary code. Vendor fix available: http://seer.support.veritas.com/docs/279085.htm Currently we are not aware of any exploits for this vulnerability.	VERITAS NetBackup Arbitrary Code Execution CVE-2005-2715	High	Secunia, Advisory: SA17181, October 13, 2005 USCERT, VU#495556

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Clam Anti-Virus ClamAV 0.87 -1	A remote Denial of Service vulnerability has been reported when handling malformed OLE2 files (e.g. DOC files). No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Clam Anti-Virus ClamAV OLE2 File Handling Denial of Service CVE-2005-3239	Low	Secunia Advisory: SA17184, October 13, 2005
Flexback up Flexbackup 1.2.1	A vulnerability has been reported due to the insecure creation of several temporary files in the default configuration, which could let a remote malicious overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Flexbackup Insecure Temporary File Creation	Medium	ZATAZ Flexbackup Advisory, October 15, 2005
Gentoo Linux Gentoo Linux	Vulnerabilities have been reported in multiple packages in Gentoo Linux due to an insecure RUNPATH vulnerability, which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200510-14.xml There is no exploit code required.	Gentoo Linux Multiple Packages Insecure RUNPATH	Medium	Gentoo Linux Security Advisory, GLSA 200510-14, October 17, 2005

GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.009-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf Sun: Updated Relief/Workaround section. **Sun: Updated Contributing Factors, Relief/Workaround, and Resolution sections.** A Proof of Concept exploit has been published.	GNU GZip Directory Traversal CVE-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.009, June 10, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005 Avaya Security Advisory, ASA-2005-172, August 29, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, Updated September 27, 2005 **Sun(sm) Alert Notification Sun Alert ID: 101816, Updated October 13, 2005**

GNU Texinfo 4.7	A vulnerability has been reported in 'textindex.c' due to insecure creation of temporary files by the 'sort_offline()' function, which could let a malicious user create/ overwrite arbitrary files. Gentoo: http://security.gentoo.org/glsa/glsa-200510-04.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/texinfo/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	GNU Texinfo Insecure Temporary File Creation CVE-2005-3011	Medium	Security Focus, Bugtraq ID: 14854, September 15, 2005 Gentoo Linux Security Advisory, GLSA 200510-04, October 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:175, October 6, 2005 Ubuntu Security Notice, USN-194-1, October 06, 2005 **SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005**

GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip/gzip Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1 Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf Sun: Updated Relief/Workaround section. **Sun: Updated Contributing Factors, Relief/Workaround, and Resolution sections.** There is no exploit code required.	GNU GZip File Permission Modification CVE-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005 Avaya Security Advisory, ASA-2005-172, August 29, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, Updated September 27, 2005 **Sun(sm) Alert Notification Sun Alert ID: 101816, Updated October 13, 2005**
Graphviz Graphviz 2.2.1	A vulnerability has been reported in '/dotty/dotty/dotty.lefty' due to the insecure creation of temporary files, which could let a malicious user overwrite arbitrary files. Update available at: http://www.graphviz.org/Download_source.php Debian: http://security.debian.org/pool/updates/main/g/graphviz/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/graphviz/** There is no exploit code required.	Graphviz Insecure Temporary File Creation CVE-2005-2965	Medium	Debian Security Advisory, DSA 857-1, October 10, 2005 **Ubuntu Security Notice, USN-208-1, October 17, 2005**

Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200503-21.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-304.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200504-07.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ FedoraLegacy: http://download.fedoralegacy.org/fedora/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	Grip CDDB Query Buffer Overflow CVE-2005-0706	High	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005 Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005 RedHat Security Advisory, RHSA-2005:304-08, March 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:066, April 3, 2005 Gentoo Linux Security Advisory, GLSA 200504-07, April 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:010, April 8, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:074 & 075, April 21, 2005 Peachtree Linux Security Notice, PLSN-0007, April 22, 2005 Fedora Legacy Update Advisory, FLSA:152919, September 15, 2005 **Conectiva Linux Announcement, CLSA-2005:1033, October 13, 2005**
Hewlett Packard Company HP-UX 11.23, B.11.23	A Denial of Service vulnerability has been reported in systems running on Itanium platforms due to a failure to properly handle exceptional conditions. Patches available at: http://itrc.hp.com Currently we are not aware of any exploits for this vulnerability.	HP-UX Itanium Denial of Service	Low	HP Security Bulletin, HPSBUX01233, October 12, 2005
Hewlett Packard Company HP-UX 10.20, B.11.11, B.11.00	A vulnerability has been reported in the FTP server included with HP-UX , which could let an unauthenticated malicious user obtain sensitive information. Reports indicate that HP has addressed this issue in HP advisory HPSBUX0208-213. There is no exploit code required; however, a Proof of Concept exploit script has been published.	HP-UX FTP Server Directory Listing	Medium	Security Focus, Bugtraq ID: 15138, October 19, 2005
Hewlett Packard Company HP-UX 10.20, B.11.11, B.11.00	A vulnerability has been reported in the LPD service, which could let a remote malicious user execute arbitrary commands. Reports indicate that HP has addressed this issue in HP advisory HPSBUX0208-213. There is no exploit code required; however, a Proof of Concept exploit script has been published.	HP-UX LPD Arbitrary Command Execution	High	Security Focus, Bugtraq ID: 15136, October 19, 2005
Hylafax Hylafax 4.2.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'xferfaxstats' script due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported because ownership of the UNIX domain socket is not created or verified, which could let a	HylaFAX Insecure Temporary File Creation CVE-2005-3069 CVE-2005-3070	Medium	Security Focus, Bugtraq ID: 14907, September 22, 2005 Gentoo Linux Security Advisory, GLSA 200509-21, September 30,

	malicious user obtain sensitive information and cause a Denial of Service. Gentoo: http://security.gentoo.org/glsa/glsa-200509-21.xml Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/h/hylafax/** There is no exploit code required.			2005 Mandriva Linux Security Update Advisory, MDKSA-2005:177, October 7, 2005 **Debian Security Advisory, DSA 865-1, October 13, 2005**
IBM AIX 5.3	Buffer overflow vulnerabilities have been reported in the 'invscout,' 'paginit,' 'diagTasksWebSM,' 'getlvname,' and 'swcons' commands and multiple 'p' commands, which could let a malicious user execute arbitrary code, potentially with root privileges. IBM has released an advisory (IBM-06-10-2005) to address this and other issues. Updated APAR availability information. Removed interim fix information. **Updated: Removed interim fix information.** Vendor fix available: http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM AIX Multiple Buffer Overflows CVE-2005-2232 CVE-2005-2233 CVE-2005-2234 CVE-2005-2235 CVE-2005-2236 CVE-2005-2237	High	Security Tracker Alert, 1014132, June 8, 2005 IBM Security Advisory, IBM-06-10-2005, June 10, 2005 Security Focus, 13909, July 7, 2005 IBM Security Advisory, September 13, 2005 **IBM Security Advisory Updated October 19, 2005**
IBM AIX 5.2.2, 5.2 L, 5.2	A vulnerability has been reported because AIX 'lscfg' command creates temporary trace files in an unsafe manner, which could let a malicious user obtain elevated privileges. Update available at: http://www-1.ibm.com/support/docview.wss?uid=isg1IY77624 There is no exploit code required.	IBM AIX LSCFG Insecure Temporary File Creation	Medium	IBM Security Advisory, IY77624, October 14, 2005
KDE KOffice 1.4.1, 1.4, 1.3-1.3.5, 1.2.1, 1.2	A buffer overflow vulnerability has been reported when handling a malformed RTF file, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.koffice.org/download/ Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/universe/k/koffice/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-12.xml** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/universe/k/koffice/** Currently we are not aware of any exploits for this vulnerability.	KDE KOffice KWord RTF Remote Buffer Overflow CVE-2005-2971	High	Security Focus, Bugtraq ID: 15060, October 11, 2005 **Ubuntu Security Notice, USN-202-1, October 12, 2005** **Gentoo Linux Security Advisory, GLSA 200510-12, October 12, 2005** **Ubuntu Security Notice, USN-202-1, October 12, 2005**
Marc Lehmann Convert-UUlib 1.50	A buffer overflow vulnerability has been reported in the Convert::UUlib module for Perl due to a boundary error, which could let a remote malicious user execute arbitrary code.	Convert-UUlib Perl Module Buffer Overflow CVE-2005-1349	High	Gentoo Linux Security Advisory, GLSA 200504-26, April 26, 2005 Secunia Advisory,

	Update available at: http://search.cpan.org/dist/Convert-UUlib/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-26.xml Debian: http://security.debian.org/pool/updates/main/libc/libconvert-uulib-perl/ SuSE: ftp://ftp.suse.com/pub/suse/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.			SA15130, April 27, 2005 Debian Security Advisory, DSA 727-1, May 20, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 **Conectiva Linux Announcement, CLSA-2005:1031, October 13, 2005**
Multiple Vendors OpenLDAP 2.1.25; Padl Software pam_ldap Builds 166, 85, 202, 199, 198, 194, 183-192, 181, 180, 173, 172, 122, 121, 113, 107, 105	A vulnerability has been reported in OpenLDAP, 'pam_ldap,' and 'nss_ldap' when a connection to a slave is established using TLS and the client is referred to a master, which could let a remote malicious user obtain sensitive information. Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-13.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/libn/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-767.html** There is no exploit code required.	Multiple Vendors TLS Plaintext Password CVE-2005-2069	Medium	Trustix Secure Linux Advisory, TSLSA-2005-0031, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-13, July 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:121, July 19, 2005 Ubuntu Security Notice, USN-152-1, July 21, 2005 Turbolinux Security Advisory, TLSA-2005-86 & 87, August 29, 2006 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 **Conectiva Linux Announcement, CLSA-2005:1027, October 14, 2005** **RedHat Security Advisory, RHSA-2005:767-8, October 17, 2005**
Multiple Vendors Cfengine 2.1.9, 2.1.8, 2.1.7 p1, 2.1.0a9, 2.1.0a8, 2.1.0a6, 2.0.1-2.0.7 p1-p3, 2.0 .8p1, 2.0 .8, 2.0 .0, 1.6 a11, 1.6 a10, 1.5.3 -4, 1.5 x; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Several vulnerabilities have been reported: a vulnerability was reported in '/bin/cfmailfilter' and '/contrib/cfcron.in' due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported in 'contrib/vicf.in/ due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/c/cfengine/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cfengine/	Cfengine Insecure Temporary Files CVE-2005-2960	Medium	Debian Security Advisories, DSA 835-1 & 836-1, October 1, 2005 Ubuntu Security Notice, USN-198-1, October 10, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:184, October 13, 2005**

Mandriva:
http://www.mandriva.com/security/advisories

There is no exploit code required.

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848 Debian:	Zlib Compression Library Buffer Overflow CVE-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1,

	http://security.debian.org/pool/updates/main/z/zsync/ Trolltech: ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz FedoraLegacy: http://download.fedoralegacy.org/fedora/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-18.xml Gentoo: http://security.gentoo.org/glsa/glsa-200509-18.xml Debian: http://security.debian.org/pool/updates/main/z/zsync/ **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-101989-1** Currently we are not aware of any exploits for this vulnerability.			2005 Security Focus, Bugtraq ID: 14162, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005 Debian Security Advisory, DSA 797-2, September 29, 2005 **Sun(sm) Alert Notification** **Sun Alert ID: 101989, October 14, 2005**
Multiple Vendors Gentoo Linux; GNU GDB 6.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdb/ http://security.ubuntu.com/ubuntu/pool/main/b/binutils/ Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-659.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-673.html http://rhn.redhat.com/errata/RHSA-2005-709.html **Avaya:** **http://support.avaya.com/elmodocs2/security/**	GDB Multiple Vulnerabilities CVE-2005-1704 CVE-2005-1705	High	Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 2005 Turbolinux Security Advisory, TLSA-2005-68, June 22, 2005 RedHat Security Advisory, RHSA-2005:659-9, September 28, 2005 RedHat Security Advisory, RHSA-2005:673-5 & RHSA-2005:709-6, October 5, 2005 **Avaya Security Advisory, ASA-2005-222, October 18, 2005**

	ASA-2005-222.pdf Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Linux kernel 2.6-2.6.14, 2.5.0-2.5.69, 2.4-2.4.32, 2.3, 2.3.x, 2.3.99, pre1-pre7, 2.2-2.2.27, 2.1, 2.1 .x, 2.1.89, 2.0.28-2.0.39	A vulnerability has been reported due to the way console keyboard mapping is handled, which could let a malicious user modify the console keymap to include scripted macro commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Linux Kernel Console Keymap Arbitrary Command Injection	Medium	Security Focus, Bugtraq ID: 15122, October 17, 2005
Multiple Vendors MandrakeSoft Multi Network Firewall 2.0, Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, Corporate Server 3.0 x86_64, 3.0; GNU wget 1.10; Daniel Stenberg curl 7.14.1, 7.13.1, 7.13, 7.12.1- 7.12.3, 7.11-7.11.2, 7.10.6- 7.10.8	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied NTLM user name data, which could let a remote malicious user execute arbitrary code. WGet: http://ftp.gnu.org/pub/gnu/wget/wget-1.10.2.tar.gz Daniel Stenberg: http://curl.haxx.se/libcurl-ntlmbuf.patch Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor WGet/Curl NTLM Username Buffer Overflow CVE-2005-3185	High	Security Tracker Alert ID: 1015056, October 13, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:182 & 183, October 13, 200 Ubuntu Security Notice, USN-205-1, October 14, 2005 Fedora Update Notifications FEDORA-2005-995 & 996, October 17, 2005 Fedora Update Notification, FEDORA-2005-1000, October 18, 2005
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2 b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELENG, 5.2 -RELEASE, 5.2, 5.1 -RELENG, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELENG, 5.0, 4.11 -STABLE, -RELENG, 4.10 -RELENG, -RELEASE, 4.10	A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security. OpenSSL: http://www.openssl.org/source/openssl-0.9.7h.tar.gz FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:21/openssl.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-800.html Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200510-11.xml **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Sun:**	Multiple Vendors OpenSSL Insecure Protocol Negotiation CVE-2005-2969	Medium	OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Mandriva Security Advisory, MDKSA-2005:179, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005 **Slackware Security Advisory, SSA:2005-286-01, October 13, 2005** **Fedora Update Notifications, FEDORA-2005-985 & 986, October 13, 2005** **Sun(sm) Alert Notification** **Sun Alert ID: 101974, October 14, 2005** **Ubuntu Security Notice, USN-204-1, October 14, 2005**

	http://sunsolve.sun.com/search/document.do?assetkey=1-26-101974-1 **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/o/openssl/** **OpenPKG:** **ftp://ftp.openpkg.org/release/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			**OpenPKG Security Advisory, OpenPKG-SA-2005.022, October 17, 2005** **SUSE Security Announcement, SUSE-SA:2005:061, October 19, 2005**
Multiple Vendors RedHat Fedora Core3; Ubuntu Linux 4.1 ppc, ia64, ia32; NTP NTPd 4.0-4.2 .0a	A vulnerability has been reported in xntpd when started using the '-u' option and the group is specified by a string, which could let a malicious user obtain elevated privileges. Upgrade available at: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/i386 /ntp-4.2.0.a.20040617-5.FC3.i386.rpm NTP: http://ntp.isc.org/Main/DownloadViaHTTP?file=ntp4/snapshots/ntp-dev/20 05/08/ntp-dev-4.2.0b-20050827.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/n/ntp/ Debian: http://security.debian.org/pool/updates/main/n/ntp/ Mandriva: http://www.mandriva.com/security/advisories **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	XNTPD Insecure Privileges CVE-2005-2496	Medium	Fedora Update Notification, FEDORA-2005-812, August 26, 2005 Ubuntu Security Notice, USN-175-1, September 01, 2005 Debian Security Advisory, DSA 801-1, September 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:156, September 6, 2005 **Conectiva Linux Announcement, CLSA-2005:1029, October 11, 2005**
Multiple Vendors SuSE Open-Enterprise-Server 9.0, Linux Enterprise Server 9; OpenWBEM 3.1 .0, 3.0.2, 2.0.14, 1.3.2	Multiple buffer overflow vulnerabilities have been reported due to insufficient bounds checking of user-supplied input before copying to insufficiently sized memory buffers, which could let a remote malicious user execute arbitrary code. SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for these vulnerabilities.	OpenWBEM Multiple Unspecified Remote Buffer Overflows	High	SUSE Security Announcement, SUSE-SA:2005:060, October 17, 2005
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Netpbm 10.0	A buffer overflow vulnerability has been reported in the 'PNMToPNG' conversion package due to insufficient bounds checking of user-supplied input before coping to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ Currently we are not aware of any exploits for this vulnerability.	NetPBM Buffer Overflow CVE-2005-2978	High	Ubuntu Security Notice, USN-210-1, October 18, 2005

Multiple Vendors XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200509-07.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-329.html http://rhn.redhat.com/errata/RHSA-2005-396.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ Mandriva: http://www.mandriva.com/security/advisories?name=MDKSA-2005:164 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/x/xfree86/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1&searchclause SUSE: ftp://ftp.suse.com/pub/suse/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101953-1 **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-218.pdf** Currently we are not aware of any exploits for this vulnerability.	XFree86 Pixmap Allocation Buffer Overflow CVE-2005-2495	High	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441 Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Debian Security Advisory DSA 816-1, September 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005 SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005 Slackware Security Advisory, SSA:2005-269-02, September 26, 2005 Sun(sm) Alert Notification Sun Alert ID: 101953, October 3, 2005 **SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005** **Avaya Security Advisory, ASA-2005-218, October 19, 2005**
Multiple Vendors xine xine-lib 1.1.0, 1.0-1.0.2, 0.9.13; Ubuntu Linux 5.0 4 powerpc, i386, amd64, ppc, ia64, ia32; Gentoo Linux	A format string vulnerability has been reported in 'input_cdda.c' when writing CD metadata retrieved from a CDDB server to a cache file, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200510-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xine-lib/	Multiple Vendors CDDB Client Format String CVE-2005-2967	High	Gentoo Linux Security Advisory, GLSA 200510-08, October 8, 200 Ubuntu Security Notice, USN-196-1, October 10, 2005 Slackware Security Advisory, SSA:2005-283-01, October 11, 2005 Mandriva Linux Security

	Slackware: ftp://ftp.slackware.com/pub/slackware/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/x/xine-lib/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** An exploit script has been published.			Update Advisory, MDKSA-2005:180, October 11, 2005 Debian Security Advisory, DSA 863-1, October 12, 2005 **Conectiva Linux Announcement, CLSA-2005:1026, October 11, 2005**
Net-SNMP Net-SNMP 5.2.1, 5.2, 5.1-5.1.2, 5.0.3 -5.0.9, 5.0.1	A remote Denial of Service vulnerability has been reported when handling stream-based protocols. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=12694&package_id=11571&release_id=338899 Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-720.html Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/net-snmp/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-395.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-225.pdf** Currently we are not aware of any exploits for this vulnerability.	Net-SNMP Protocol Denial of Service CVE-2005-2177	Low	Secunia Advisory: SA15930, July 6, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Fedora Update Notifications, FEDORA-2005-561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:720-04, August 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:137, August 11, 2005 Ubuntu Security Notice, USN-190-1, September 29, 2005 RedHat Security Advisory, RHSA-2005:395-18, October 5, 2005 **Conectiva Linux Announcement, CLSA-2005:1032, October 13, 2005** **Avaya Security Advisory, ASA-2005-225, October 18, 2005**
Net-snmp Net-snmp 5.x	A vulnerability has been reported in 'fixproc' due to a failure to securely create temporary files in world writeable locations, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code with ROOT privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-18.xml Fedora:	Net-SNMP Fixprox Insecure Temporary File Creation CVE-2005-1740	High	Gentoo Linux Security Advisory, GLSA 200505-18, May 23, 2005 Fedora Update Notifications, FEDORA-2005-561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:373-23,

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: https://rhn.redhat.com/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-395.html **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-225.pdf** There is no exploit code required.			September 28, 2005 RedHat Security Advisory, RHSA-2005:395-18, October 5, 2005 **Avaya Security Advisory, ASA-2005-225, October 18, 2005**
Padl Software pam_ldap Build 179, Build 169	A vulnerability has been reported when handling a new password policy control, which could let a remote malicious user bypass authentication policies. Upgrades available at: ftp://ftp.padl.com/pub/pam_ldap.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200508-22.xml **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-767.html** There is no exploit code required.	PADL Software PAM_LDAP Authentication Bypass CVE-2005-2641	Medium	Bugtraq ID: 14649, August 24, 2005 US-CERT VU#778916 Gentoo Linux Security Advisory, GLSA 200508-22, August 31, 2005 **Conectiva Linux Announcement, CLSA-2005:1027, October 14, 2005** **RedHat Security Advisory, RHSA-2005:767-8, October 17, 2005**
PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ Ubuntu: http://security.ubuntu.	PCRE Regular Expression Heap Overflow CVE-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02 , August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2,

	com/ubuntu/ pool/main/ Debian: http://security.debian. org/pool/updates/ main/p/pcre3/ SUSE: ftp://ftp.SUSE.com/ pub/SUSE Slackware: ftp://ftp.slackware.com/ pub/slackware/ slackware-10.1/ testing/packages/ php-5.0.5/php- 5.0.5-i486-1.tgz Gentoo: http://security.gentoo. org/glsa/glsa- 200509-08.xml Conectiva: ftp://atualizacoes. conectiva.com.br/ 10/ Gentoo: http://security.gentoo .org/glsa/glsa- 200509-12.xml Debian: http://security.debian. org/pool/updates/ main/p/python2.2/ Gentoo: http://security.gentoo. org/glsa/glsa- 200509-19.xml Debian: http://security.debian. org/pool/updates/ main/p/python2.3/ Conectiva: ftp://atualizacoes. conectiva.com.br/ 10/ TurboLinux: ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ia32/ **Avaya:** **http://support.avaya.com/ elmodocs2/security/ ASA-2005-216.pdf** Currently we are not aware of any exploits for this vulnerability.			2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 Slackware Security Advisory, SSA:2005-251-04, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005 Conectiva Linux Announce-ment, CLSA-2005:1009, September 13, 2005 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Debian Security Advisory, DSA 817-1 & DSA 819-1, September 22 & 23, 2005 Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005 Debian Security Advisory, DSA 821-1, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-92, October 3, 2005 **Avaya Security Advisory, ASA-2005-216, October 18, 2005**
phpMyAdmin phpMyAdmin 2.6.4 -pl1	A vulnerability has been reported in 'libraries/grab_ globals.lib.php' due to insufficient verification of the 'subform' array parameter before including files, which could let a malicious user include arbitrary files. **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200510-16.xml** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPMyAdmin File Include	Medium	Secunia Advisory: SA17137, October 11, 2005 **Gentoo Linux Security Advisory, GLSA 200510-16, October 17, 2005**
slocate slocate 2.7	A Denial of Service vulnerability has been reported when a specially crafted directory structure that contains long paths is submitted. Mandriva: http://www.mandriva. com/security/	slocate Long Path Denial of Service CVE-2005-2499	Low	Mandriva Linux Security Update Advisory, MDKSA-2005:147, August 22, 2005 Turbolinux Security Advisory, TLSA-2005-91,

	advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: https://rhn.redhat.com/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-346.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.			September 20, 2005 RedHat Security Advisory, RHSA-2005:345-24, September 28, 2005 RedHat Security Advisory, RHSA-2005:346-19, October 5, 2005 **Conectiva Linux Announcement, CLSA-2005:1028, October 11, 2005**
Sun Microsystems Inc. Solaris 10.0, _x86, 9.0, _x86, 8.0, _x86, 7.0, _x86	A vulnerability has been reported in the Xsun and Xprt commands due to an unspecified error, which could let a malicious user obtain elevated privileges. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101800-1 **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-220.pdf** Currently we are not aware of any exploits for this vulnerability.	Sun Solaris Xsun & Xprt Elevated Privileges CVE-2005-3099	Medium	Sun(sm) Alert Notification Sun Alert ID: 101800, September 26, 2005 **Avaya Security Advisory, ASA-2005-220, October 18, 2005**
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'privilege management' feature due to an unspecified error; and a vulnerability was reported in the Process File System (procfs) due to an unspecified security issue, which could let a malicious user obtain sensitive information. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101895-1 http://sunsolve.sun.com/search/document.do?assetkey=1-26-101949-1 There is no exploit code required.	Sun Solaris Denial of Service & Information Disclosure CVE-2005-3250	Medium	Sun(sm) Alert Notifications, Sun Alert ID: 101895 & 101949, October 12, 2005
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0	A Denial of Service vulnerability has been reported in the '/proc' filesystem. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101987-1 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris Proc Filesystem Denial of Service	Low	Sun(sm) Alert Notification Sun Alert ID: 101987, October 14, 2005
Sun Microsystems, Inc. Solaris 9.0, _x86, 8.0, _x86	A Denial of Service vulnerability has been reported due to an unspecified error in the UFS (Unix File System). Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101940-1 **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-219.pdf** Currently we are not aware of any exploits for this vulnerability.	Sun Solaris UFS Local Denial of Service CVE-2005-3071	Low	Sun(sm) Alert Notification Sun Alert ID: 101940, September 22, 2005 **Avaya Security Advisory, ASA-2005-219, October 18, 2005**

University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/ Debian: http://security.debian.org/pool/updates/main/u/uw-imap/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-10.xml **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	High	Secunia, Advisory: SA17062, October 5, 2005 Debian Security Advisory, DSA 861-1, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 **US-CERT VU#933601** **SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005**
xloadimage xloadimage 4.1	A buffer overflow vulnerability has been reported when handling the title of a NIFF image when performing zoom, reduce, or rotate functions, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/x/xloadimage/ http://security.debian.org/pool/updates/main/x/xli/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-802.html** Currently we are not aware of any exploits for this vulnerability.	Xloadimage NIFF Image Buffer Overflow CVE-2005-3178	High	Debian Security Advisories, DSA 858-1 & 859-1, October 10, 2005 **RedHat Security Advisory, RHSA-2005:802-4, October 18, 2005**
YaPiG YaPig 0.95 b	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'Website' field when adding a comment, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability was reported in 'view.php' due to insufficient sanitization of the 'img_size' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because users can perform certain actions via HTTP POST requests without validity checks, which could let a remote malicious user perform certain administrative tasks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Yapig Cross-Site Scripting & HTTP POST Requests Validity	Medium	Technical University of Vienna Security Advisory TUVSA-0510-001, October 13, 2005
Yukihiro Matsumoto Ruby 1.6 - 1.6.8, 1.8 - 1.8.2	A vulnerability has been reported in 'eval.c' due to a flaw in the logic that implements the SAFE level checks, which could let a remote malicious user bypass access restrictions to execute scripting code. Patches available at: ftp://ftp.ruby-lang.org/pub/ruby/1.6/1.6.8-patch1.gz Updates available at:	Ruby Safe Level Restrictions Bypass CVE-2005-2337	Medium	Security Tracker Alert ID: 1014948, September 21, 2005 US-CERT VU#160012 Gentoo Linux Security Advisory, GLSA 200510-05, October 6, 2005 Ubuntu Security Notice,

	http://www.ruby-lang.org/patches/ruby-1.8.2-xmlrpc-ipimethods-fix.diff Gentoo: http://security.gentoo.org/glsa/glsa-200510-05.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/ Debian: http://security.debian.org/pool/updates/main/r/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-799.html** **Debian:** **http://security.debian.org/pool/updates/main/r/ruby1.8/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.		USN-195-1, October 10, 2005 Debian Security Advisories, DSA 860-1 & DSA 862-1, October 11, 2005 **RedHat Security Advisory, RHSA-2005:799-3, October 11, 2005** **Debian Security Advisory, DSA 864-1, October 13, 2005** **Conectiva Linux Announcement, CLSA-2005:1030, October 13, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Abi Source Community AbiWord 2.2.0-2.2.10, 2.2.12, 2.0.1-2.0.9	Multiple stack-based buffer overflow vulnerabilities have been reported due to insufficient bounds checking of user-supplied data prior to copying it to an insufficiently sized memory buffer while importing RTF files, which could let a remote malicious user execute arbitrary code. The vendor has addressed this issue in AbiWord version 2.2.11. Users are advised to contact the vendor to obtain the appropriate update. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/abiword/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Currently we are not aware of any exploits for these vulnerabilities.	AbiWord Stack-Based Buffer Overflows CVE-2005-2972	High	Ubuntu Security Notice, USN-203-1, October 13, 2005 Fedora Update Notification, FEDORA-2005-989, October 13, 2005
Accelerated Mortgage Manager Accelerated Mortgage Manager	An SQL injection vulnerability has been reported in the 'Password' field due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	Accelerated Mortgage Manager SQL Injection	Medium	Security Focus, Bugtraq ID: 15097, October 13, 2005
AdventNet ManageEngine NetFlow Analyzer 4.0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	NetFlow Analyzer Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15127, October 18, 2005

Australian Projects Pty Limited Trust Digital Trusted Mobility Suite 3.0, 2.0	A vulnerability has been reported because a malicious user can bypass authentication policies. No workaround or patch available at time of publishing. There is no exploit code required.	Trust Digital Trusted Mobility Suite Authentication Bypass	Medium	Security Focus, Bugtraq ID: 15109, October 14, 2005
Cisco Systems Cisco IOS 12.2ZH & 12.2ZL based trains, 12.3 based trains, 12.3T based trains, 12.4 based trains, 12.4T based trains	A buffer overflow vulnerability has been reported in the authentication proxy, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml Rev. 1.1: Added 12.2SG, 12.2SEC, and 12.2SXF releases to Software Version and Fixes table. Rev. 1.2: In Software Versions and Fixes table: 12.2ZH changed to 12.2SH, added 12.2ZF. **Revision 1.3** **Updated Exploitation and Public Announcements section and all 12.2 references in Affected Products.** Currently we are not aware of any exploits for this vulnerability.	Cisco IOS Firewall Authentication Proxy Buffer Overflow CVE-2005-2841	High	Cisco Security Advisory, Document ID: 66269, September 7, 2005 US-CERT VU#236045 Cisco Security Advisory, Document ID: 66269 Rev 1.1 & 1.2, September 22 & 26, 2005 **Cisco Security Advisory, Document ID: 66269 Rev 1.3, October 12, 2005**
Cisco Systems CSS11500 Content Services Switch 7.30 (00.09)S, 7.30 (00.08)S, 7.20 (03.10)S, 7.20 (03.09)S, 7.10 (05.07)S, 7.5, 7.4	A remote Denial of Service vulnerability has been reported when processing malformed SSL client certificates. Updates available at: http://www.cisco.com/warp/public/707/cisco-sa-20051019-css.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco 11500 Content Services Switch Malformed SSL Client Certificate Remote Denial of Service	Low	Cisco Security Advisory, Document ID: 67919, October 19, 2005
Complete PHP Counter Complete PHP Counter	An SQL injection & Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code and HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploits have been published.	Complete PHP Counter SQL Injection & Cross-Site Scripting	Medium	Security Tracker Alert ID: 1015054, October 13, 2005
Computer Associates Message Queuing software prior to 1.07 Build 220_13 & 1.11 Build 29_13	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the Computer Associates Message Queuing (CAM) service due to an unspecified error when specially crafted packets are submitted to the TCP port; buffer overflow vulnerabilities were reported due to unspecified boundary errors, which could lead to the execution of arbitrary code; and a vulnerability was reported due to a failure in the CAM service to verify the legitimacy of the CAFT application, which could let a remote malicious user spoof a legitimate CAFT instance and ultimately execute arbitrary code. Upgrade information available at: http://supportconnectw.ca.com/public/ca_common_docs/camsecurity_notice.asp **An exploit script has been published.**	Computer Associates Message Queuing Multiple Vulnerabilities CVE-2005-2667 CVE-2005-2668 CVE-2005-2669	High	Computer Associates Advisory, August 19, 2005 US-CERT VU#619988 **Security Focus, Bugtraq ID: 14622, October 19, 2005**
e107.org e107 website system 0.6172, 0.6171, 0.617	An SQL injection vulnerability has been reported in 'resetcore.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	E107 SQL Injection	Medium	Security Focus, Bugtraq ID: 15125, October 18, 2005
Gallery Gallery 2.0 Beta1-Beta3, 2.0 Alpha-Alpha4, 2.0	A Directory Traversal vulnerability has been reported in the 'main.php' script due to insufficient sanitization of the 'g2_itemID' parameter, which could let a remote malicious user obtain sensitive information. Updates available at:	Gallery Directory Traversal CVE-2005-3251	Medium	Security Tracker Alert ID: 1015060, October 14, 2005

	http://codex.gallery2.org/index.php/Gallery2:Download There is no exploit code required; however, a Proof of Concept exploit has been published.			
Hitachi TP1/Server Base	A remote Denial of Service vulnerability has been reported due to a failure to properly handle malformed data. Patch information available at: http://www.hitachi-support.com/security_e/vuls_e/HS05-020_e/01-e.html Currently we are not aware of any exploits for this vulnerability.	Hitachi TP1/Server Base Remote Denial of Service	Low	Hitachi Security Advisory, HS05-020, October 13, 2005
IBM DB2 Universal Database for Windows 8.1.9 a, 8.1.9, 8.1.8 a, 8.1.8, 8.1.7 b, 8.1.7, 8.1.6 c, 8.1.6, 8.1.5, 8.1.4, 8.1, 8.0, DB2 Universal Database for Solaris 8.1.9 a, 8.1.9, 8.1.8 a, 8.1.8, 8.1.7 b, 8.1.7, 8.1.6 c, 8.1.6, 8.1.5, 8.1.4, 8.1, 8.0, DB2 Universal Database for Linux 8.1.9 a, 8.1.9, 8.1.8 a, 8.1.8, 8.1.7 b, 8.1.7, 8.1.6 c, 8.1.6, 8.1.5, 8.1.4, 8.1, 8.0, DB2 Universal Database for HP-UX 8.1.9 a, 8.1.9, 8.1.8 a, 8.1.8, 8.1.7 b, 8.1.7, 8.1.6 c, 8.1.6, 8.1.5, 8.1.4, 8.1, 8.0 , DB2 Universal Database for AIX 8.1.9 a, 8.1.9, 8.1.8 a, 8.1.8, 8.1.7 b, 8.1.7, 8.1.6 c, 8.1.6, 8.1.5, 8.1.4, 8.1, 8.0	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported when handling SQL queries that contain constant strings; a Denial of Service vulnerability was reported when processing hash joins; a Denial of Service vulnerability was reported in 'db2agents' due to an error when handling abnormally terminated connections; a vulnerability was reported when handling object creations due to an error, which could let a malicious user create objects based on routines even when the user is not granted execute privileges; a Denial of Service vulnerability was reported in the 'in' list or the 'SYSCAT.TABLES' when handling a query that contains more than 32000 elements; and a Denial of Service vulnerability was reported in the 'db2jd' listener service when handling connections from certain clients. Updates available at: http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24010283 Currently we are not aware of any exploits for these vulnerabilities.	IBM DB2 Universal Database Denials of Service & Security Restriction Bypass	Medium	Secunia Advisory: SA17031, October 18, 2005
Mozilla.org Thunderbird 1.5 Beta 2, 1.0.7	A vulnerability has been reported due to an insecure SMTP authentication protocol negotiation, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Mozilla Thunderbird Insecure SMTP Authentication Protocol Negotiation	Medium	Security Focus, Bugtraq ID: 15106, October 14, 2005
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/	Firefox Multiple Vulnerabilities CVE-2005-2260 CVE-2005-2261 CVE-2005-2262 CVE-2005-2263 CVE-2005-2264 CVE-2005-2265 CVE-2005-2267 CVE-2005-2269 CVE-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798

Gentoo:
ftp://security.gentoo.org/glsa/

Mandriva:
http://www.mandriva.com/security/advisories

Fedora:
http://download.fedora.redhat.com/pub/fedora/linux/core/updates

RedHat:
http://rhn.redhat.com/errata/RHSA-2005-586.html

Slackware:
http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880

Ubuntu:
http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/

http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/

http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/

SUSE:
ftp://ftp.suse.com/pub/suse/

Debian:
http://security.debian.org/pool/updates/main/m/mozilla-firefox/

http://security.debian.org/pool/updates/main/m/mozilla/

SGI:
ftp://patches.sgi.com/support/free/security/advisories/

Gentoo:
http://security.gentoo.org/glsa/glsa-200507-24.xml

Slackware:
ftp://ftp.slackware.com/pub/slackware/

Debian:
http://security.debian.org/pool/updates/main/m/mozilla-firefox/

Debian:
http://security.debian.org/pool/updates/main/m/mozilla/

Fedora:
http://download.fedoralegacy.org/fedora/

HP:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01229

Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005

Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005

SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005

Debian Security Advisory, DSA 775-1, August 15, 2005

SGI Security Advisory, 20050802-01-U, August 15, 2005

Debian Security Advisory, DSA 777-1, August 17, 2005

Debian Security Advisory, DSA 779-1, August 20, 2005

Debian Security Advisory, DSA 781-1, August 23, 2005

Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005

Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005

Slackware Security Advisory, SSA:2005-085-01, August 28, 2005

Debian Security Advisory, DSA 779-2, September 1, 2005

Debian Security Advisory, DSA 810-1, September 13, 2005

Fedora Legacy Update Advisory, FLSA:160202, September 14, 2005

HP Security Bulletin, HPSBOV01229, September 19, 2005

HP Security Bulletin, HPSBUX01230, October 3, 2005

Ubuntu Security Notice, USN-155-3, October 04, 2005

Sun(sm) Alert Notification
Sun Alert ID: 101952, October 17, 2005

HP:
http://www.hp.com/
products1/unix/
java/mozilla/index.html

Ubuntu:
http://security.ubuntu.com/
ubuntu/pool/main/
m/mozilla-locale-da/

Sun:
**http://sunsolve.sun.com/
search/document.do?
assetkey=1-26-101952-1**

Exploits have been published.

Mozilla.org Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6; Mozilla Browser 1.7.11; Mozilla Thunderbird 1.0.6	A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code. Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-769.html http://rhn.redhat.com/errata/RHSA-2005-768.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ HP: http://software.hp.com/ Mandriva: http://www.mandriva.com/security/advisories **HPSBUX01231 Rev1: Preliminary Mozilla 1.7.12 available.** **Netscape: http://browser.netscape.com/ns8/download/default.jsp** A Proof of Concept exploit script has been published.	Mozilla/Netscape/ Firefox Browsers Domain Name Buffer Overflow CVE-2005-2871	High	Security Focus, Bugtraq ID: 14784, September 10, 2005 RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005 Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005 Ubuntu Security Notice, USN-181-1, September 12, 2005 US-CERT VU#573857 Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005 Security Focus, Bugtraq ID: 14784, September 22, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200509-11:02, September 29, 2005 Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Debian Security Advisory, DSA 837-1, October 2, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 HP Security Bulletin, HPSBUX01231, October 3, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005 **HP Security Bulletin, HPSBUX01231 Rev 1, October 12, 2005**
Multiple Vendors Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11; **Netscape Browser 8.0.3.3**	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability	Mozilla Browser / Firefox Multiple Vulnerabilities CVE-2005-2701 CVE-2005-2702 CVE-2005-2703	High	Mozilla Foundation Security Advisory, 2005-58, September 22, 2005 RedHat Security Advisory,

was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability was reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandriva:	CVE-2005-2704 CVE-2005-2705 CVE-2005-2706 CVE-2005-2707		RHSA-2005:789-11, September 22, 2005 Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 SGI Security Advisory, 20050903-02-U, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005 Gentoo Linux Security Advisory [UPDATE] , September 29, 2005 SUSE Security Announcement, SUSE-SA:2005:058, September 30, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Debian Security Advisory, DSA 838-1, October 2, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005 Ubuntu Security Notice, USN-200-1, October 11, 2005 **Security Focus, Bugtraq ID: 14916, October 19, 2005**

	http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ **Netscape:** **http://browser.netscape.com/ns8/download/default.jsp** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Snort Project Snort 2.4.0-2.4.2; Nortel Networks Threat Protection System Intrusion Sensor 4.1, Nortel Networks Threat Protection System Defense Center 4.1	A buffer overflow vulnerability has been reported in the Back Orifice processor due to a failure to securely copy network-derived data into sensitive process buffers, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Snort Back Orifice Preprocessor Remote Buffer Overflow CVE-2005-3252	High	Internet Security Systems Protection Advisory, October 18, 2005 Technical Cyber Security Alert TA05-291A, October 18, 2005 US-CERT VU#175500
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; AbiSource Community AbiWord 2.2 .0-2.2.9, 2.0.1-2.0.9	A buffer overflow vulnerability has been reported in the RTF importer due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.abisource.com/downloads/abiword/2.2.10/source/abiword-2.2.1 0.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/abiword/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-20.xml **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	AbiWord RTF File Processing Remote Buffer Overflow CVE-2005-2964	High	Security Tracker Alert ID: 1014982, September 28, 2005 Ubuntu Security Notice, USN-188-1, September 29, 2005 Fedora Update Notification, FEDORA-2005-955, September 30, 2005 Gentoo Linux Security Advisory, GLSA 200509-20, September 30, 2005 **Conectiva Linux Announcement, CLSA-2005:1035, October 14, 2005** **SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005**
Multiple Vendors University of Kansas Lynx 2.8.6 dev.1-dev.13, 2.8.5 dev.8, 2.8.5 dev.2-dev.5, 2.8.5, 2.8.4 rel.1, 2.8.4, 2.8.3 rel.1, 2.8.3 pre.5, 2.8.3 dev2x, 2.8.3 dev.22, 2.8.3, 2.8.2 rel.1, 2.8.1, 2.8, 2.7; RedHat Enterprise Linux WS 4, WS 3, 2.1, ES 4, ES 3, ES 2.1, AS 4, AS 3, AS 2.1, RedHat Desktop 4.0, 3.0, RedHat Advanced Workstation for the Itanium Processor 2.1 IA64	A buffer overflow vulnerability has been reported in the 'HTrjis()' function when handling NNTP article headers, which could let a remote malicious user execute arbitrary code. University of Kansas Lynx: http://lynx.isc.org/current/lynx2.8.6dev.14.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-803.html	Lynx 'HTrjis()' NNTP Remote Buffer Overflow CVE-2005-3120	High	Gentoo Linux Security Advisory, GLSA 200510-15, October 17, 2005 Ubuntu Security Notice, USN-206-1, October 17, 2005 RedHat Security Advisory, RHSA-2005:803-4, October 17, 2005 Fedora Update Notifications, FEDORA-2005-993 & 994, October 17, 2005 Mandriva Linux Security Update Advisory,

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/10/ A Proof of Concept Denial of Service exploit script has been published.			MDKSA-2005:186, October 18, 2005 Conectiva Linux Announcement, CLSA-2005:1037, October 19, 2005
MySource MySource 2.14.0RC2, 2.14 .0	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient verification of some input before used to include files, which could let a remote malicious user include arbitrary files; and Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of some input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://mysource.squiz.net/download/downloads/download_2.14.2 There is no exploit code required; however, Proof of Concept exploits have been published.	MySource Cross-Site Scripting & File Inclusion	High	Secunia Advisory: SA16946, October 18, 2005
OpenSSH OpenSSH 4.1, 4.0, p1	Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials. Upgrades available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-4.2.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-527.html Mandriva: http://www.mandriva.com/security/advisories **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/o/openssh/** **Conectiva:** **ftp://atualizacoes.**	OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials CVE-2005-2797 CVE-2005-2798	Medium	Secunia Advisory: SA16686, September 2, 2005 Fedora Update Notification, FEDORA-2005-858, September 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005 Slackware Security Advisory, SSA:2005-251-03, September 9, 2005 Fedora Update Notification, FEDORA-2005-860, September 12, 2005 RedHat Security Advisory, RHSA-2005:527-16, October 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:172, October 6, 2005 **Ubuntu Security Notice, USN-209-1, October 17, 2005** **Conectiva Linux Announcement, CLSA-2005:1039, October 19, 2005**

	conectiva.com.br/10/ There is no exploit code required.			
Opera Software Opera Web Browser 8.0-8.0 2, 7.50-7.54, 7.20-7.23, 7.11, j, b, 7.10, 7.0 win32 Beta 1&2, 7.0 win32, 7.0 3win32, 7.0 2win32, 7.0 1win32, 6.10 linux, 6.0.2 win32-6.0.5 win32, 6.0.3 linux, 6.0.2 linux, 6.0.1 win32, 6.0.1 linux, 6.0.1, 6.0 win32, 6.0 6, 6.0 .6win32, 6.0, 5.12 win32, 5.12, 5.1 1 win32, 5.1 0 win32, 5.0 2 win32, 5.0 Mac, 5.0 Linux, 8 Beta 3	A remote Denial of Service vulnerability has been reported when parsing certain malformed HTML content. No workaround or patch available at time of publishing. Proof of Concept exploits have been published.	Opera Web Browser Malformed HTML Parsing Remote Denial of Service	Low	Security Focus, Bugtraq ID: 15124, October 17, 2005
Oracle Corporation JD Edwards EnterpriseOne 8.x, OneWorld 8.x; Oracle Application Server 10g, Collaboration Suite Release 1, 2, Database 8.x, Database Server 10g, Developer Suite 10g, E-Business Suite 11i, Enterprise Manager 10.x, 9.x, Oracle9i Application Server, Oracle9i Database Enterprise Edition, Oracle9i Database Standard Edition, Workflow 11.5.9 .5, 11.5.1; PeopleSoft Enterprise Customer Relationship Management (CRM) 8.x, EnterpriseOne Applications 8.x	85 vulnerabilities have been reported in various Oracle products. Some have an unknown impact, and others can be exploited to conduct SQL injection attacks, Cross-Site Scripting attacks, or potentially to compromise a vulnerable system. Patch information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html Currently we are not aware of any exploits for these vulnerabilities.	Oracle October Security Update	High	Oracle Critical Patch Update, October 18, 2005 Technical Cyber Security Alert TA05-292A, October 19, 2005 US-CERT VU#210524
PHP Group PHP 5.0.5, 4.4.0	A vulnerability has been reported in the 'open_basedir' directive due to the way PHP handles it, which could let a remote malicious user obtain sensitive information. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/php4/** There is no exploit code required.	PHP 'Open_BaseDir' Information Disclosure CVE-2005-3054	Medium	Security Focus, Bugtraq ID: 14957, September 27, 2005 **Ubuntu Security Notice, USN-207-1, October 17, 2005**
PHP PHP 5.0.5	Multiple vulnerabilities have been reported which could let a remote malicious user bypass the 'safedir' directory restriction. These issues have been addressed in the latest CVS. Users are advised to contact the vendor to obtain updates. There is no exploit code required; however, Proof of Concept exploits have been published.	PHP Safedir Restriction Bypass	Medium	Security Focus, Bugtraq ID: 15119, October 17, 2005
PHPNUke PHPNuke 7.9, 7.8	A Directory Traversal vulnerability has been reported in 'Modules.php' due to insufficient sanitization, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://securityreason.com/download/1/4 There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPNuke Remote Directory Traversal	Medium	Security Reason Alert, October 19, 2005
phpWeb site phpWebsite 0.10.1, 0.10, 0.9.3-1-0.9.3 -4, 0.9.3, 0.8.3, 0.8.2, 0.7.3	An SQL injection vulnerability was reported in the search module due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patches available at: http://osdn.dl.sourceforge.net/sourceforge/phpwebsite/	PHPWebSite Search Module SQL Injection	Medium	Security Focus, Bugtraq ID: 15088, October 12, 2005

	phpwebsite_security_patch_20051012.tgz There is no exploit code required; however a Proof of Concept exploit and exploit script has been published.			
PunBB PunBB 1.2.1-1.2.8	An SQL injection vulnerability has been reported in 'search.php' due to insufficient sanitization of the 'old_searches' array parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available at: http://www.punbb.org/downloads.php There is no exploit code required; however, a Proof of Concept exploit has been published.	PunBB SQL Injection	Medium	KAPDA New advisory #6, October 14, 2005
RTasarim WebAdmin RTasarim WebAdmin	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	RTasarim WebAdmin Login SQL Injection	Medium	Security Focus, Bugtraq ID: 15107, October 14, 2005
Stani's Python Editor SPE 0.7.5	A vulnerability has been reported because files belonging to SPE are installed with world-writable permissions, which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200510-13.xml There is no exploit code required.	SPE Insecure File Permissions	Medium	Secunia Advisory: SA17224, October 17, 2005 Gentoo Linux Security Advisory, GLSA 200510-13, October 15, 2005
Symantec Brightmail Anti-Spam 6.0-6.0.2	A remote Denial of Service vulnerability has been reported due to a failure to properly handle certain malformed MIME content. Patches available at: ftp:ftp://ftp.symantec.com/public/english_us_canada/products/sba/sba_60x/updates/ There is no exploit code required.	Symantec Brightmail AntiSpam Remote Denial of Service	Low	Symantec Security Advisory, SYM05-019, October 12, 2005
W-Agora W-Agora 4.2	Several vulnerabilities have been reported: a vulnerability was reported in 'extras/quicklist.php' due to insufficient verification of the 'site' parameter before used to include files, which could let a malicious user include arbitrary files; and a vulnerability was reported in 'browse_avatar.php' because arbitrary files can be uploaded inside the web root, which could let a malicious user execute arbitrary PHP script code. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script has been published.	W-Agora File Inclusion & File Upload	High	Secunia Advisory: SA17201, October 17, 2005
WebGUI WebGUI 6.6.0- 6.7.5, 6.5.0-6.5.6, 6.4.0, 6.3.0	A vulnerability has been reported due to an unspecified error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/pbwebgui/webgui-6.7.6-gamma.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	WebGUI Unspecified Arbitrary Code Execution	High	Security Focus, Bugtraq ID: 15083, October 12, 2005
Xeobook Xeobook 0.93	Multiple HTML injection vulnerabilities have been reported due to insufficient sanitization of input passed to various fields when signing the guestbook, which could let a remote malicious user execute arbitrary script code. No workaround or patch available at time of publishing. There is no exploit code required.	Xeobook Multiple HTML Injection	Medium	Secunia Advisory: SA17159, October 12, 2005
Xerver Xerver 4.17	Several vulnerabilities have been reported: a vulnerability was reported because a remote malicious user can obtain the source code of script files when appending a dot to the filename in an HTTP request; and a vulnerability was reported because a remote malicious user can obtain the content of a directory even when there is an index file by	Xerver Multiple Input Validation Vulnerabilities	Medium	Secunia Advisory: SA17243, October 19, 2005

	appending a null character to the path in a HTTP request. Upgrade available at: http://www.javascript.nu/xerver/ There is no exploit code required; however, Proof of Concept exploits have been published.			
XMail XMail 1.21	A buffer overflow vulnerability has been reported in the 'AddressFromAtPtr()' function due to a boundary error when copying the hostname portion of an e-mail address to a 256-byte buffer, which could let a malicious user execute arbitrary code. Upgrade available at: http://www.xmailserver.org/ Currently we are not aware of any exploits for this vulnerability.	XMail Command Line Buffer Overflow CVE-2005-2943	High	Security Tracker Alert ID: 1015055, October 13, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Microsoft creates virtual Wi-Fi:** Microsoft has developed a technique to allow people to access multiple Wi-Fi networks with a single Wi-Fi card. Virtual Wi-Fi is designed to improve multitasking, save money on hardware and reduce the power needed for Wi-Fi communications. The software is designed to run with Windows XP. Source: http://www.vnunet.com/vnunet/news/2144172/microsoft-creates-virtual-wi.
- **Mobile phone security comes with a swagger:** VTT, a Finnish electronics firm, has unveiled a biometric security system for mobile phones that operates by measuring the user's gait. The device, which contains movement sensors, connects to a phone and is calibrated so that it recognizes the unique walking pattern of its owner. Source: http://www.vnunet.com/vnunet/news/2144116/system-locks-mobiles-user-walk
- **New Hacker Targets: Cell Phones And PDAs:** There was a time when the biggest mobile computing risk was losing a laptop, but things have changed. Cell phones, smart phones, and PDAs increasingly are being used to access business applications, E--mail, and the Internet. New security threats to mobile devices that store and distribute company information are emerging. They're becoming victims of zombie attacks and other forms of hacking; malware; hybrid PC--mobile viruses like Comwarrior, Bluejacking, and Cabir; and spam. Many businesses are finding they need plans for securing mobile devices, including what methods to use and rules for how devices can be used. Source: http://www.securitypipeline.com/news/172301486;jsessionid=XGKC2CBBHNDQGQSNDBECKH0CJUMEKJVN.
- **Securing laptop PCs for public Wi-Fi hot spots:** Cranite Systems, a California-based network security company, said it has new technology that could enable government employees to work securely on laptop computers and other devices from public Wi-Fi hot spots or networks at home. They announced that their SafeConnect product would provide the first Layer 2 secure access solution for enterprise networks. The patent-pending technology would also allow remote users to access the same functions they use when working in an office. Source: http://www.fcw.com/article91132-10-17-05-Web
- **Newest Mobile Devices Are Latest Threat To Network Security:** Next-generation mobile devices may enhance mobile workers' productivity, but they also place unprecedented demands on enterprise security infrastructure. Until stronger security practices become more widespread, enterprise mobile devices will continue to represent a threat to sensitive corporate data. Next-generation mobile handsets are capable of using different types of wireless networks, and they're being powered by a growing number of mobile operating systems. Source: http://www.mobilepipeline.com/trends/172301056

Wireless Vulnerabilities

- WifiScanner-1.0.0.tar.gz: WifiScanner is an analyzer and detector of 802.11b stations and access points which can listen alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.
- rfakeap-0.1.tar.gz: Proof of Concept code for a program that emulates IEEE 802.11 access points thanks to wireless raw injection. It aims at creating/injecting both beacon and probe response frames in order to emulate valid IEEE 802.11 access points.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
October 19, 2005	cacam_logsecurity_win32.pm	Yes	Exploit for the Computer Associates Message Queuing Multiple Vulnerabilities.
October 19, 2005	ewdd.pdf	N/A	Exploiting Windows Device Drivers is a paper that describes device driver exploitation techniques, and provides detailed descriptions of techniques used. It also includes full exploit code with sample vulnerable driver code for testing purposes.
October 19, 2005	hpux_ftpd_preauth_list.pm	Yes	Proof of Concept exploit for the HP-UX FTP Server Directory Listing vulnerability.
October 19, 2005	hpux_lpd_exec.pm	Yes	Proof of Concept exploit for the HP-UX LPD Arbitrary Command Execution vulnerability.

October 19, 2005	qcrack-v0.1.tgz	N/A	A program written to test the security of md5 passwords by attempting to brute force them. The user can also specify the characters to use when brute-forcing.
October 19, 2005	rfakeap-0.1.tar.gz	N/A	Proof of Concept code for a program that emulates IEEE 802.11 access points thanks to wireless raw injection. It aims at creating/injecting both beacon and probe response frames in order to emulate valid IEEE 802.11 access points.
October 19, 2005	rsa_iiswebagent_ redirect.pm	Yes	Exploit for the RSA Authentication Agent for Web Buffer Overflow Vulnerability.
October 18, 2005	e017_xpl.php e107remote.txt	No	Proof of Concept exploits for the E107 Resetcore.PHP SQL Injection vulnerability.
October 17, 2005	0xletzdance.c winrar-3.50-eng.txt	No	Scripts that exploit the RARLAB WinRAR Command Line Processing Buffer Overflow vulnerability.
October 14, 2005	lynx-data.zip	Yes	A Proof of Concept Denial of Service exploit for the Lynx 'HTrjis()' NNTP Buffer Overflow vulnerability.
October 14, 2005	wagora_420_xpl.php wagora420_xpl.txt	No	Scripts that exploit the W-Agora Multiple Arbitrary PHP Code Injection Vulnerabilities.
October 13, 2005	suckit2priv.tar.gz	N/A	An easy-to-use, Linux-i386 kernel-based rootkit.
October 13, 2005	typsoft-1.11-DOS.pl	No	Script that exploits the TYPSoft FTP Server RETR Denial of Service Vulnerability.
October 13, 2005	WifiScanner-1.0.0.tar.gz	N/A	An analyzer and detector of 802.11b stations and access points which can listen alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.
October 12, 2005	phpwebsite-sql-inj.pl	Yes	Script that exploits the PHPWebSite Search Module SQL Injection Vulnerability.

[back to top]

Trends

- **Snort flaw leaves systems vulnerable:** The U.S. Computer Emergency Readiness Team (CERT) announced that the open source IDS software, widely deployed in corporations and governments, was vulnerable to a buffer overflow in the preprocessor component it uses to detect the Back Orifice Trojan. Source: http://www.securityfocus.com/brief/17.
- **DDoS attacks still biggest threat:** According to a survey of global ISPs from Arbor Networks in their Worldwide ISP Security Report, companies should devote more resources to countering Distributed Denial of Service (DDoS) attacks when investing in security. Questionnaires were sent to 36 large ISPs in the US, Europe and Asia. Source: http://www.techworld.com/security/news/index.cfm?NewsID=4570.
- **Ten-Minute Guide To Killing Network Malware:** According to Forrester Research,"If you ask any company why it has invested in anti-spyware tools, the first thing they'll say is that every PC was running so slowly that they couldn't function." Source: http://www.networkingpipeline.com/172301862.
- **U.S. insists on controlling Web:** According to a top U.S. official, the United States refuses to relinquish its role as the Internet's principal traffic policeman. They are rejecting calls in a United Nations meeting for a U.N. body to take over. But while the United States stuck to its position, other negotiators said there was a growing sense that a compromise had to be reached and that no single country ought to be the ultimate authority over such a vital part of the global economy. Source: http://www.cnn.com/2005/TECH/internet/09/30/internet.control.ap/index.html.
- **Report: Anti-spam push helping curb U.S. junk mail:** According to Sophos, the United States continues to be the world's worst source of spam, but computers are relaying far fewer junk e-mails than a year ago. The spam volume from South Korea and China is substantially up, compared with the same period last year. The report covered Sophos's analysis of messages received in its scanning network between April and September this year. The United States was the country of origin for around 26 percent of global spam, down from 41.5 percent a year ago. The share of spurious e-mails from South Korea and China, which held the second and third position, has gone up to nearly 20 percent and 16 percent respectively, from 12 percent and 9 percent. Source: http://news.com.com/Report+Antispam+push+helping+curb+U.S.+junk+mail/2100-7349_3-5894104.html?tag=cd.top.
- **FFIEC Releases Guidance on Authentication in Internet Banking Environment:** The Federal Financial Institutions Examination Council (FFIEC) has released guidance on the risks and risk management controls that are necessary to authenticate Internet-based financial services customer identity. The guidance, Authentication in an Internet Banking Environment, was issued to reflect the many significant legal and technological changes with respect to the protection of customer information, increasing incidents of identity theft and fraud, and the introduction of improved authentication technologies and other risk mitigation strategies. Source: http://www.ffiec.gov/press/pr101205.htm.
- **A sophisticated Trojan-worm hybrid threatens users' privacy and their bank accounts, reports Panda Software:** PandaLabs has reported the appearance of a new kind of hybrid malware that has both worm and Trojan features, which could be used to steal confidential information of any kind, such as banking information, personal details or other type of information entered in Web registration forms. This Eyeveg.D is a sophisticated hybrid with two sides to it: it carries out Trojan actions against the infected computer, and acts as a worm to spread. Source: http://www.net-security.org/press.php?id=3524.
- **Antiphishing Efforts Show Success:** According to the Anti-Phishing Working Group (APWG) the number of days a phishing site remains online has dropped to an average of 5.5 days. This is a sign that countermeasures against fraudulent web sites are being enacted with increased speed. Source: http://news.yahoo.com/s/pcworld/20051014/tc_pcworld/123027.
- **Websense's Web Security Trends Report Finds Marked Increase in Crimeware and Malicious Websites :** Websense, Inc. released its 2005 Semi-Annual Web Security Trends Report. According to the report, the web continued to evolve and grow as an attack vector in the first half of 2005 and there was a marked increase in the number of malicious websites and in the amount of "crimeware", a term which refers to using malicious code written with criminal intent. Source: http://www.securitypark.co.uk/pfv.asp?articleid=24437.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
5	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
7	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
10	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.

Table updated October 17, 2005

[back to top]

Last updated October 20, 2005